.2600

AUGUST, 1985

VOLUME TWO, NUMBER EIGHT

2600 is published by 2600 Enterprises, Inc., an electronoysary organization. Subscription rates: $12—1 year, individual. $30—1 year, corporate. $1 per back issue. Overseas: $20—1 year. Lifetime subscription: $250. Corporate sponsorship: $2600. Make checks payable to: 2600 Enterprises, Inc. Write to: 2600, Box 752, Middle Island, NY 11953-0752. Dial: 5167512600. BBS: 2013664431. ISSN: 0749-3851. Write to Box 762, Middle Island, NY 11953-0762 for advertising rates and article submissions.

SEIZED!

2600 *Bulletin Board is Implicated in Raid on Jersey Hackers*

On July 12, 1985, law enforcement officials seized the Private Sector BBS, the official computer bulletin board of *2600* magazine, for "complicity in computer theft," under the newly passed, and yet untested, New Jersey Statute 2C:20-25. Police had uncovered in April a credit carding ring operated around a Middlesex County electronic bulletin board, and from there investigated other North Jersey bulletin boards. Not understanding subject matter of the Private Sector BBS, police assumed that the sysop was involved in illegal activities. Six other computers were also seized in this investigation, including those of Store Manager who ran a BBS of his own, Beowolf, Red Barchetta, the Vampire, NJ Hack Shack, sysop of the NJ Hack Shack BBS, and that of the sysop of the Treasure Chest BBS.

Immediately after this action, members of *2600* contacted the media, who were completely unaware of any of the raids. They began to bombard the Middlesex County Prosecutor's Office with questions and a press conference was announced for July 16. The system operator of the Private Sector BBS attempted to attend along with reporters from *2600*. They were effectively thrown off the premises. Threats were made to charge them with trespassing and other crimes. An officer who had at first received them civilly was threatened with the loss of his job if he didn't get them removed promptly. Then the car was chased out of the parking lot. Perhaps prosecutor Alan Rockoff was afraid that the presence of some technically literate reporters would ruin the effect of his press release on the public. As it happens, he didn't need our help.

The next day the details of the press conference were reported to the public by the press. As Rockoff intended, paranoia about hackers ran rampant. Headlines got as ridiculous as hackers ordering tank parts by telephone from TRW and moving satellites with their home computers in order to make free phone calls. These and even more exotic stories were reported by otherwise respectable media sources. The news conference understandably made the front page of most of the major newspapers in the US, and was a major news item as far away as Australia and in the United Kingdom due to the sensationalism of the claims. We will try to explain why these claims may have been made in this issue.

On July 18 the operator of The Private Sector was formally charged with "computer conspiracy" under the above law, and released in the custody of his parents. The next day the American Civil Liberties Union took over his defense. The ACLU commented that it would be very hard for Rockoff to prove a conspiracy just "because the same information, construed by the prosecutor to be illegal, appears on two bulletin boards," especially as Rockoff admitted that "he did not believe any of the defendants knew each other." The ACLU believes that the system operator's rights were violated, as he was assumed to be involved in an illegal activity just because of other people under investigation who happened to have posted messages on his board.

In another statement which seems to confirm Rockoff's belief in guilt by association, he announced the next day that "630 people were being investigated to determine if any used their computer equipment fraudulently." We believe this is only the user list of the NJ Hack Shack, so the actual list of those to be investigated may turn out to be almost 5 times that. The sheer overwhelming difficulty of this task may kill this investigation, especially as they find that many hackers simply leave false information. Computer hobbyists all across the country have already been called by the Bound Brook, New Jersey office of the FBI. They reported that the FBI agents used scare tactics in order to force confessions or to provoke them into turning in others. We would like to remind those who get called that there is nothing inherently wrong or illegal in calling *any* BBS, nor in talking about *any* activity. The FBI would not comment on the case as it is an "ongoing investigation" and in the hands of the local prosecutor. They will soon find that many on the Private Sector BBS's user list are data processing managers, telecommunications security people, and others who are interested in the subject matter of the BBS, hardly the underground community of computer criminals depicted at the news conference. The Private Sector BBS was a completely open BBS, and police and security people were even invited on in order to participate. The BBS was far from the "elite" type of underground telecom boards that Rockoff attempted to portray.

Within two days, Rockoff took back almost all of the statements he made at the news conference, as AT&T and the DOD discounted the claims he made. He was understandably unable to find real proof of Private Sector's alleged illegal activity, and was faced with having to return the computer

(continued on page 2-51)

COMMENTARY: THE THREAT TO US ALL

We're very used to reporting on this kind of a story. We've done it so many times in our pages that we're tempted to gloss over "raid" stories because they've become so commonplace. But we realize that we cannot ever ignore such events, because we all need to know what is happening out there. It's really not a pretty sight.

Mention the word computer to someone and you'll see a variety of reactions. In our case it would be overwhelming enthusiasm, much like an explorer confronting a new adventure. But to many people, computers are evil and scary. This takes two forms: fear of the computers themselves, and complete ignorance as to what they and their operators are capable of doing. We saw plenty of the latter last month.

We don't care if people refuse to understand computers and how they fit in. What we do object to, however, is when these same people insist on being the ones to pass laws and define abuses concerning computers. In every investigation we have seen, ignorance abounds. True, such ignorance can be amusing -- we all got a good laugh when we heard the New Jersey authorities insisting that the hackers were moving satellites "through the blue heavens" But losing The Private Sector isn't at all funny, and whether you were a caller to that bulletin board or not, its loss is a very troubling sign.

What was The Private Sector? Picture a sounding board of ideas, theories, and experiences and you'll have a good idea. The Private Sector was a place to ask questions, talk to experts, and learn a hell of a lot about high technology. It was *never* a place to trade illegal information, such as Sprint codes, credit card numbers, or computer passwords. The system operator took elaborate measures to ensure this, such as going through each and every message, public and private, on a daily basis to make sure nothing shady was transpiring. We don't believe he should have had to do even this. We can't condone censorship of any kind -- our feelings were that if people wanted to do illegal things, then *they* would face the consequences, not the people who simply talked to them. But the sysop had his own policy and he stuck by it and kept the board clean. He wanted two things: a good, interesting bulletin board and no trouble with authorities. At least he managed to obtain one of those goals.

Again we see ignorance and a disregard towards the rights of all of us. They came and took our board, whose only "crime" was being mentioned on another board that had been raided the month before. The Private Sector was completely innocent of any wrongdoing. Yet it is being held at this moment, without bail. See the connection to free speech yet? Many people have trouble seeing this because of that word computer. Yet a computer bulletin board is probably the purest form of free speech that exists today. Anyone can call, anyone can speak. True identity is not required. Why should this be considered a threat in a democracy?

We've been told there is legislation pending in the House of Representatives to "regulate" bulletin boards. What this would mean is a re-definition of BBS's into a sort of public utility. The system operator would have to take full responsibilty for everything that was posted. (This means if he went away for a week and didn't censor messages, he could find himself facing charges when he came back!) The system operator would also be *required* to confirm the identities of all users and we wouldn't at all be surprised if part of this involves the paying of some sort of fee for a license. These sound very much like the kind of tactics used by repressive regimes to curb public assemblies and newspapers. Is this in fact what is happening? Aren't bulletin boards a form of public assembly, a kind of electronic publication?

Before all of the computer hobbyists out there start hating the "hackers" for ruining the future of bulletin boards, we'd like for them to view this whole affair as an important and inevitable test. True, some boards today are being used for sleazy things and criminals are involved. One could say the same thing about telephones or even cars. (Think of how much illegal information must be passed within the confines of some people's cars.) The fact is we cannot sacrifice a freedom simply because some bad people are using it.

We see this sort of test frequently. When police pull you over and ask all kinds of questions when you haven't done anything wrong, you probably wind up fairly annoyed. But when they say it's a way of catching drunk drivers -- well, now that's different. A little bit of freedom isn't all that important when the public welfare is at stake. What rubbish! And what a perfect way to start eroding our rights as individuals.

We're glad that we were able to convince the American Civil Liberties Union to take the case, which is most likely their introduction to the issues that surround the use of computers. We've found good media like *The New York Times* that actually cares about what is said in their stories and attempts to find out what all the sides are. We've also seen sensationalism at its worst, such as WABC-TV, which took our comments out of context and made us seem like an anti-hacker establishment! Or *The New York Daily News* reporter who asked us after we said the system operator was "surprised" to see his computer taken, "Was he *shocked*?" Most of all, though, we're amazed at the response of hackers and non-hackers alike, who came to the defense of The Private Sector, offering services, equipment, advice. Our phones have been jammed -- we've never seen anything like this. Everyone who called The Private Sector knows it was devoid of all the things it's being accused of having. The most important thing anyone can do at this point is to make sure *everyone* knows. The concept of a bulletin board must be understood. The value of The Private Sector must be known. The connection to publications and freedom of speech has to be established so that people understand the threat to *them* whenever a bulletin board is shut down. When we do this, we'll be that much closer to getting The Private Sector back on line and making a positive precedent.

2600 A Hacking Victim

2600 News Service

When we received our June SBS Skyline bill, we were a bit surprised. Over six hundred dollars of it came from calls we never made. But what's really interesting is the way that the Skyline people handled it. In early June, we got a call telling us that their sophisticated equipment detected hackers trying to guess a code by scanning numerically. They said our code would soon be discovered, so they were going to give us a new one, with two extra digits added. They did this and that very day our old code was inactivated. The illegal calls had occurred *before* that day, and we figure Skyline must have known this. Maybe they thought that *2600*, in our corporate clumsiness, would pay a huge bill without investigation. Many big companies would. Gotta give them credit for trying.

When we called up about it, they didn't want to handle it over the phone! "Send the bill through the mail," they said. "Mark the calls you made and deduct the rest." Why are phone companies so afraid to do things over the phone?

As long as Skyline decided to give the "perpetrators" some extra time before the investigation starts, we figure we might as well lend a hand too. Our old code was 880099. We loved that code and are very upset at losing it. Our new eight digit one is very difficult to remember and nowhere near as fun.

And one last note about those new eight digit numbers. Phone phreaks have *already* figured out a way around them. If you dial the first six digits of an eight digit code, then the ten digit phone number and hit a # key, you'll get your tone back! That means there are only a hundred possible codes since there are only two more digits to figure out and one of them *definitely* works! If you enter six digits that are not part of an eight digit code, and then a ten digit phone number, you'll get an error message immediately or that fake carrier tone Skyline loves to send out. That tone, incidentally, is for you hackers with Apples and Commodores that scan all night long looking for the code that will get you through to a number that responds with a carrier tone. In the morning, you see how many carrier detects you got and which codes got them for you. Skyline's idea is that if *every* invalid code gives a hacker a carrier tone, there is no way for a computer to separate the good codes from the bad ones. Come on! How about setting your computer to dial a *non*-carrier and telling it to print out only those codes that *didn't* get a carrier tone? And there are probably a hundred more ways. Big corporations can be *so* much fun.

New Phone System For Courthouse

New Brunswick Home News

The Middlesex County Courthouse and Administration Building will have a new phone system installed to increase the security of the complex, according to Middlesex County Prosecutor Alan J. Rockoff. [Yes, the same Alan J. Rockoff that was convinced computer hackers were moving satellites through the "blue heavens".]

The phone system, due by September, will be able to detect and cut off unauthorized calls made in an emergency situation.

"Once a phone is activated it will show up on this massive diagram that will be on a computer screen and will show where that phone is being used in the courthouse or the administration building," Rockoff said.

The system would monitor which phones were active and would be able to cut connections in an instant. Rockoff promised that the system would not be designed to tap phones. [Of course, if his knowledge of tapping is anything like his knowledge of satellites....]

Seizure of Private Sector

(continued from page 2-49)

equipment with nothing to show for his effort. Rockoff panicked, and on July 31, the system operator had a new charge against him, "wiring up his computer as a blue box." Apparently this was referring to his Novation Applecat modem which is capable of generating any hertz tone over the phone line. By this stretch of imagination an Applecat could produce a 2600 hertz tone as well as the MF which is necessary for "blue boxing." However, each and every other owner of an Applecat or any other modem that can generate its own tones therefore has also "wired up his computer as a blue box" by merely installing the modem. This charge is so ridiculous that Rockoff probably will never bother to press it. However, the wording of *wiring up the computer* gives Rockoff an excuse to continue to hold onto the computer longer in his futile search for illegal activity.

"We have requested that the prosecutors give us more specific information," said Arthur Miller, the lawyer for The Private Sector. "The charges are so vague that we can't really present a case at this point." Miller will appear in court on August 16 to obtain this information. He is also issuing a demand for the return of the equipment and, if the prosecutors don't cooperate, will commence court proceedings against them. "They haven't been particularly cooperative," he said.

Rockoff probably will soon reconsider taking Private Sector's case to court, as he will have to admit he just didn't know what he was doing when he seized the BBS. The arrest warrant listed only "computer conspiracy" against Private Sector, which is much more difficult to prosecute than the multitude of charges against some of the other defendants, which include credit card fraud, toll fraud, the unauthorized entry into computers, and numerous others.

Both Rockoff and the ACLU mentioned the Supreme Court in their press releases, but he will assuredly take one of his stronger cases to test the new New Jersey computer crime law. By seizing the BBS just because of supposed activities discussed on it, Rockoff raises constitutional questions. Darrell Paster, a lawyer who centers much of his work on computer crime, says the New Jersey case is "just another example of local law enforcement getting on the bandwagon of crime that has come into vogue to prosecute, and they have proceeded with very

(continued on page 2-56)

moving satellites right up in the blue...

(When the details of the Middlesex County Prosecutor's Office press conference hit the newspapers the next day, the ridiculous charges made many people knowledgeable about technology and computers very disgusted. Many simple and innocent bits of information had been twisted into "evidence" of illegal activities. With the aid of The Shadow, we have put together a guide to these misinterpretations in the hopes that everyone can see how this investigation has gotten completely out of control.)

One of the more sensationalist of the crimes of the hackers was, as Middlesex County Prosecutor Alan Rockoff said, "changing the positions of satellites up in the blue heavens" and causing communications satellites to "change positions" in order to make free phone calls "possibly disrupting intercontinental communications and making legitimate phone calls impossible." This story was twisted by the media to the extent of dire predictions of hackers causing satellites to crash into the Soviet Union, provoking a nuclear war, as heard on one Wednesday morning radio news program, and the "disruption of telex and telephone transmission between two continents." Very soon afterwards AT&T and Comsat denied that any attempts to re-route satellites had been made. In fact, an AT&T executive on the MacNeil-Lehrer Report stated that the computers which controlled the satellites weren't even connected with the phone lines and that the satellites were constantly monitored for movement, and none had ever been detected.

So how did this fallacy arise? Not having been on the other boards we can only assume that they may have contained information on making illegal international calls, giving the police the idea that there was international phreaking. Many long distance companies use satellites to transmit their calls. The Private Sector BBS had much information on satellites, fitting in with its purpose as a telecommunications information source. One recurring topic was TASI, (Time Assignment Speech Interpolation) a method of transmitting satellite conversations. TASI is only the packet switching of telephone conversations, where the conversation is converted into small packets and sent over satellite and many long distance circuits effectively simultaneously along with many other conversations. TASI permits several conversations to be sent over one satellite circuit, thus permitting more conversations without sending up more satellites. It is comparable to talking about modem transmission methods. As far as we know there is *no* way to use TASI and similar information fraudulently, and certainly one cannot move satellites using this. Evidently Middlesex County law enforcement saw posted messages on the routing of calls *through* a satellite and jumped, due to paranoia, to the conclusion it was for the *moving* of the satellites.

Another of the more sensationalist charges was that the youths had Department of Defense "secret telephone codes" that could enable them to penetrate the Pentagon. Due to the subject matter of the Private Sector BBS (telecommunications), AUTOVON, the DoD's private telephone network, was often brought up because it offers an extremely interesting network architecture quite different than civilian phone systems. Some AUTOVON phone numbers were on the board as examples of the format of the unique numbering plan. These numbers are easy to obtain and have appeared on other boards. These AUTOVON phone numbers can be obtained from a declassified DoD phone book available from the Government Printing Office for a small fee.

One of the more muddled of the ch es was reported by media sources vari ly as hackers "ordering tank parts using stolen credit cards by computer from TRW", breaking into TRW computers for top secret information on tank parts, and other variations. It turns out that TRW does do some defense contracting, but it has nothing at all to do with tank parts, instead making automobile parts for various non-tank military vehicles. TRW does have a credit rating service accessable by computer, but this is in a completely separate division. Somehow the authorities and the press had mangled the different alleged crimes of credit card fraud and the breaking into of a defense contractor's computer system which happened to have defense department information in it. Since TRW is in both credit ratings *and* defense contracting, it would be an obvious jump in illogic to have the hackers break into TRW computers and order tank parts by credit card.

And just why was the Private Sect discussing TRW in the first place? TRW's credit rating computers were discussed on the Private Sector much as TRW was discussed in *2600* (July 1984). Since people's private credit information is stored under shoddy security, it naturally came up in the discussion of computer security as a particularly bad instance. Such discussions weren't for the purpose of breaking into computer systems, but were conducted by various hackers (*not* computer criminals) and data processing managers who were interested in security methods and computer abuses.

Another possible source of confusion is the fact that many of the messages on the BBS's that were confiscated were written by people 13 years old or younger. People this age may brag and tell stories as young people sometimes do. We're sure that you can imagine a young person telling his friends how he blew up an AT&T computer or knocked a satellite out of orbit, much the same way he might brag about the speed of his father's new sports car. It would be quite irresponsible of authorities to issue the kid's father a ticket based on this just as it was irresponsible of them to announce to the press the list of computer crimes without verifying that actual crimes did occur. The authorities are still unsure what crimes, if any, actually took place.

When all these exotic charges are revealed to be mere flights of fancy, a great lack of knowledge about computers and telephony is uncovered on the part of law enforcemer We feel that law enforcement official along with telecommunications hobbyists, should start to research the field by look-

...what was really going on?

ing in their public library, or even better a local college library (under 621 Dewey Decimal). Several magazines also provide good information, such as *Telecom Digest*, *Communications Age*, as well as *2600* and other telecom industry publications.

Credit Card Fraud Explained

With regards to the credit card part of this whole thing here is a brief guide to how credit card numbers are used fraudulently.

First one obtains a complete credit card number including expiration date. If a driver's license number, social security number, or other information is also obtained, then it is easier to use the credit card number to charge goods and services. Credit and other information is usually found in the form of carbons (actual carbon paper that fits between the credit slip and the receipt) that are often discarded after their use. Carbons contain all of the information from a previous legitimate purchase. If someone is required to include their address or social security number with their credit card number then this will also appear on the carbon which is found in the daily trash of many retail stores. One can then call up a company that takes charge requests over the phone and order goods using the credit card information that was found with the trash.

But the real hurdle to committing credit card fraud is to have the package delivered and for this one needs a mailing address. This can be obtained a few ways. One is to get a post office box under an assumed name, and another is to have it delivered to a place where it can be picked up before the package is noticed. By using stolen or false identification or by being convincing to a postal clerk, one can obtain a post office box. One can also ask for general post office delivery, where the post office will put your package on the racks behind the counter waiting for you to pick up. By finding a vacant or temporarily empty home one can also have the objects delivered there.

And this is how it is done from start to finish. There may be more effective ways to complete the various stages, but all in all it is that simple. This is mainly because companies make it easy to make a purchase while only supplying a small amount of personal information. Often if a company has been guaranteed that it will be covered for the value of fraudulently charged goods, then the company will make it easier for a person to charge them.

The problem of credit card fraud has a few simple cures: make it harder to order objects by phone (companies can issue a code that must be verbally communicated in order to complete the purchase--one that *doesn't* appear on the carbon) or discontinue the use of carbons in credit card receipts. There are many other safeguards that can be used to decrease this type of fraud.

This section was not intended to be a guide in how to commit a crime, but an edification of how this crime is *not* committed. Credit card fraud is not high tech crime. No computer is involved or has to be involved; no illegal phone calls are involved; and it is not necessary to break into TRW or other credit bureaus to commit this crime.

Computers may be used as notepads or message boards where individuals might write down the information that they found in the trash. With regards to credit card fraud, computers are only used as a medium for communication. Credit card carbons are so easily found and the process of performing the actual illegal charge has been made so easy that it is not even necessary to discuss the topic with others to be able to commit the crime.

Because of the use of US mail or post office boxes, the post office is involved in investigating this type of crime. The Secret Service was authorized last October to investigate credit card fraud. The FBI has a variety of reasons to investigate. There are already laws everywhere against credit card fraud, and there are already associated penalties. It is nothing new to law enforcement. In addition, much of all credit card fraud is committed by those who steal, manufacture, or find whole credit cards.

We hope that this thorough explanation will help to get rid of those inaccurate stories we've seen abounding. Again we'd like to clarify that law enforcement people should learn a bit about computers and telecommunications and above all try to control their enthusiasm.

We are, of course, only qualified to comment on the specific case of The Private Sector. We feel that Rockoff and his cohorts will have to search a long time for the "special codes that provided illegal access to the information at issue" on The Private Sector, as they just aren't there.

Latest news:

```
+-----------------------------------------+
!                                         !
!   System News Posted:     05-29-85      !
!                                         !
+-----------------------------------------+

RULES OF THIS BBS:
------------------

1) NO CODES/PASSWORDS/CC #'s are to be
   posted or exchanged via E-mail.
   Violation of this rule will cost you
   your access. Remember we see every-
   thing you type.

2) POST INFORMATION relating to telecom
   ONLY!

These rules are to protect both you the
user and we the sysops.

   If you have any interesting articles
please send them to 2600 via Email to
"2600 MAGAZINE"  We appreciate all good
and informative articles.
```

WHY COMPUTERS GET SNATCHED

When a computer system is confiscated from a young person because they break into someone's mainframe, because they have a BBS with lots of codes or passwords posted on it, or because they are caught making illegal phone calls, no one complains. It is often said that the young person obviously commited a crime and deserves to lose their computer. The kid's parents are not going to complain, because they know enough to think twice about arguing with the FBI, The Secret Service, or whomever. Plus the parents do not want to make headlines in the local papers. So what the authorities in effect are doing is convicting people and punishing them by taking away their computer system. This is, in part, due to the fact that charges are often not pressed against young people who break into computers.

When one asks some big company's public relations department whether or not people break into their computers they are likely to say: "Oh no, of course not, we have the most secure systems." This is because it looks bad to admit to security breaches in one's system; one's livelihood. In the case of GTE-Telemail, the people there saw something going wrong, told the FBI and then the case was out of their hands. A full four months or more after the raids in October, 1983 the default password was still the letter "A". And it was not until weeks after this was publicized that this was corrected (see *2600*, April 1984). Obviously Telemail did not want to admit that they were reluctant to deal with the real problem. TRW was upset last summer when the press (see *2600*, July 1984) had to tell the world about breaches into the company's credit gathering system.

These companies make money because their systems are reliable and secure and not because they will prosecute people who break in. They know that it is not worth it to try to prosecute kids, and it is better to prosecute those who try to use a computer to embezzle. In addition kids are often exempt from prosecution or, because of youthful offender laws, will have little or no penalties placed against them.

It is for these reasons that it is more advantageous for companies to have authorities confiscate equipment and punish the hacker that way rather than dragging them through court. They keep the equipment by calling it evidence in an ongoing investigation, and they often return it if the kid tells them everything they know. (In addition, the kid's confession about the poor security of whatever system he may have broken into is rarely related to the proper security personnel at the company that owns the system.) This is also a form of harassment or scare tactics. Aren't young people citizens and don't they have rights just like the rest of us? They have the right to due process and have to be proven guilty beyond a reasonable doubt.

Law enforcement types have said that they occasionally have to make hacking headlines in order to reduce the amount of late night computer activity. They have admitted that they need to get a good bust in before the summer starts, because they know that all young people with computers may spend their summer trying to start World War III from their home. And this is a no-no.

Some Important Questions To Ask

All these events raise many questions: Who is responsible for a BBS? If it is the sysop how about remote sysops? How much can one do to regulate a BBS? On the Private Sector messages were regularly scanned for potential illegal material and then deleted when found. Then the user who posted the message was denied any further access. What more can one do than this? Especially if the BBS is simply a hobby and not a full time job. On the Private Sector it was extremely unlikely to see a credit card number or an Allnet code. Plus isn't it really illegal to *use* these codes? This is because a crime has been comm ed only after a code has been used. But n again in some states, namely California, it is illegal to tell people code formats. This makes all credit card commercials, sample credit cards, and this publication illegal there. Does this sound right?

It also raises a variety of questions on the admissibility of electronic evidence. The Middlesex prosecutors consider reading messages on a BBS the same as overhearing a conversation. Is this the proper way to look at BBS messages? And what about electronic mail? Is the sysop responsible for the contents of electronic mail just because he provides the service? Isn't it just as sacred as US mail? Now, there are currently no laws that require court approval in order to tap data lines. So, how does one consider evidence that is received by a legal, yet unapproved tap? If authorities can confiscate a suspect computer system because it has an illegal message on it, why don't they confiscate Compuserve when it is used by criminals to exchange illegal information? Or is the government just upset about the fact that people are communicating in an unregulated manner? These questions go on and on. What are the answers?

Some of the answers are only starting to appear as legislators address the problems that are connected with the computer age. But often they are only responses to headlines. For instance, we were told that Senator Paul Trible (R-Virginia) has recently proposed legislation (S-1305) that would regulate obscene material on a BBS. Called the "Computer Pornography and Child Exploitation Prevention Act of 1985," the legislation would prohibit the posting of names or addresses of children and prevent discussion that could be construed as pertaining to child exploitation. A couple of explicit messages might give sufficient cause to get a warrant to seize your BBS. We have not seen the legislation itself yet, but it was related to us by Jerry Berman of the American Civil Liberties Union's Privacy Project in Washington. He said that this showed "Congress trying to regulate an industry that no one understands and that has no constituency." This is all too true.

On the other side, Berman told us about legislation that is being drafted by Patrick Leahy (D-Vermont) that would extend laws which limit wiretaps in order to protect data transmission, electronic mail, and BBS's. This is something that would be harder to get through Congress, as reduces the power of law enforcement.

We will try to keep you informed when anything new happens. So ask the questions now, before they are answered for you.

HOW CAN SYSOPS PROTECT THEMSELVES?

A wave of anxiety is sweeping across the nation as BBS operators wonder if they'll be next, and BBS users worry about whether or not their names will show up in raided userlogs. As we've now seen, it makes no difference whether or not you're actually engaged in illegal activity. Any bulletin board anywhere could be next and there's not all that much that can be done to prevent it. Not until we get some laws passed to protect *us*.

In the meantime, however, there are a few suggestions we can pass along to either lessen the odds of a raid or to thwart the invaders before they manage to get into confidential material.

Obviously, if you have a bulletin board that frequently posts codes and passwords, you can almost expect to get visited, even if it's only being done in private mail. What's very important at this stage is the role the system operator is playing with regards to this information. If he/she is an active participant, there will most certainly be an attempt to make an example of them. It's similar to draft registration evaders who publicize their opposition--they are the ones that get prosecuted, not the ones who keep a low profile about it. By running a bulletin board, you are calling attention to yourself, so it stands to reason that you should keep your act clean.

Had this article been written before July 12, we would have advised sysops to encourage people not to post credit card numbers, passwords, etc. in order not to get hassled. But this is no longer the case. With The Private Sector, authorities moved in *even though* the board was kept spanking clean of the above. So now, the only way we can guarantee that your board won't be snatched from you is if you unplug it and put it in a closet. Using a bulletin board for communication between two or more people can now be considered risky.

Assuming that you still want your board up, there are other precautionary measures. For one thing, the boards that ask the caller whether or not they work for law enforcement really are working against themselves. First off, do they honestly expect all law enforcement types to dutifully say yes and never call back when they're denied access? Do they really think that these people can't get their foot in the door even if it is an "elite" board? Even if there is nothing illegal on such a board, attention is drawn to it by such statements and it will become impossible to persuade the authorities that there simply isn't a higher access level. On the same token, sysops that run a disclaimer with words to the effect of "the sysop takes no responsibility for what is said on this board" are kidding themselves if they think this is going to save them from harassment. Those words *should* apply, naturally, but at the moment they don't seem to.

Whether or not you want to censor the messages on your system is up to you. Sometimes it helps to weed out undesirables and sometimes it's an intrusion into someone's privacy. We never liked the practice, although it was done regularly on The Private Sector. It's your board and you have the right to run it your way.

What really needs to be addressed at this point is the concept of protection. Yes, you have the right to protect yourself against thugs that come into your home, no matter who sent them. One way is by scrambled data. There are many scrambling programs around and some of them are quite good; even the NSA would have a time cracking the code. We feel that all userlogs should be scrambled, at the very least. (In some cases, a valid form of protection would be to keep no userlog at all.) System operators should try to figure out a way to scramble everything so that nothing is available to unauthorized parties. When raids become totally fruitless, maybe then they will stop. Of course, now there is the problem of being forced, under penalty of law, to unscramble everything. A vivid imagination can probably find a way around this as well.

The best method of protection is complete destruction of data. Some people hook up their computers so that if the wrong door is opened or a button isn't pressed, a magnet activates and wipes the disk clean. Bookies like to do this with their Apples. Similar systems can be rigged so that if a computer is unplugged, the first thing it does upon revival is a purge (not a directory purge which comes with simply deleting file names, a complete reformatting of the disk which erases *all* data). This means, though, that every power failure will have the same effect. It will take some time to make a good system of protection, but this is probably the most constructive project that BBS operators can engage in. It doesn't matter if you have "nothing to hide". The fact is you have everything to protect from intruding eyes. Because when they seize equipment they read everything without concern that the sysop may be the caretaker of people's personal messages and writings.

We'd like to hear other methods of outsmarting these goons. It's not very hard. For instance, you could have a bulletin board dial-in at one location, which will then call-forward to the real location, or still another dummy location. Each of these requires another phone line, but you'll get plenty of warning, especially if a dummy computer is set up at one of the locations. And this is only the beginning.

We don't enjoy having to suggest these courses of action. We'd like very much to be able to get on with what we're supposed to be doing: discussing telecommunications and computers in our own way. Instead we have to pause again to defend our right to say these things. It's a necessary course of action and, if we hold our heads up, it will be a successful one.

HOW CAN SYSOPS PROTECT THEMSELVES?

A wave of anxiety is sweeping across the nation as BBS operators wonder if they'll be next, and BBS users worry about whether or not their names will show up in raided userlogs. As we've now seen, it makes no difference whether or not you're actually engaged in illegal activity. Any bulletin board anywhere could be next and there's not all that much that can be done to prevent it. Not until we get some laws passed to protect *us*.

In the meantime, however, there are a few suggestions we can pass along to either lessen the odds of a raid or to thwart the invaders before they manage to get into confidential material.

Obviously, if you have a bulletin board that frequently posts codes and passwords, you can almost expect to get visited, even if it's only being done in private mail. What's very important at this stage is the role the system operator is playing with regards to this information. If he/she is an active participant, there will most certainly be an attempt to make an example of them. It's similar to draft registration evaders who publicize their opposition--they are the ones that get prosecuted, not the ones who keep a low profile about it. By running a bulletin board, you are calling attention to yourself, so it stands to reason that you should keep your act clean.

Had this article been written before July 12, we would have advised sysops to encourage people not to post credit card numbers, passwords, etc. in order not to get hassled. But this is no longer the case. With The Private Sector, authorities moved in *even though* the board was kept spanking clean of the above. So now, the only way we can guarantee that your board won't be snatched from you is if you unplug it and put it in a closet. Using a bulletin board for communication between two or more people can now be considered risky.

Assuming that you still want your board up, there are other precautionary measures. For one thing, the boards that ask the caller whether or not they work for law enforcement really are working against themselves. First off, do they honestly expect all law enforcement types to dutifully say yes and never call back when they're denied access? Do they really think that these people can't get their foot in the door even if it is an "elite" board? Even if there is nothing illegal on such a board, attention is drawn to it by such statements and it will become impossible to persuade the authorities that there simply isn't a higher access level. On the same token, sysops that run a disclaimer with words to the effect of "the sysop takes no responsibility for what is said on this board" are kidding themselves if they think this is going to save them from harassment. Those words *should* apply, naturally, but at the moment they don't seem to.

Whether or not you want to censor the messages on your system is up to you. Sometimes it helps to weed out undesirables and sometimes it's an intrusion into someone's privacy. We never liked the practice, although it was done regularly on The Private Sector. It's your board and you have the right to run it your way.

What really needs to be addressed at this point is the concept of protection. Yes, you have the right to protect yourself against thugs that come into your home, no matter who sent them. One way is by scrambled data. There are many scrambling programs around and some of them are quite good; even the NSA would have a time cracking the code. We feel that all userlogs should be scrambled, at the very least. (In some cases, a valid form of protection would be to keep no userlog at all.) System operators should try to figure out a way to scramble everything so that nothing is available to unauthorized parties. When raids become totally fruitless, maybe then they will stop. Of course, now there is the problem of being forced, under penalty of law, to unscramble everything. A vivid imagination can probably find a way around this as well.

The best method of protection is complete destruction of data. Some people hook up their computers so that if the wrong door is opened or a button isn't pressed, a magnet activates and wipes the disk clean. Bookies like to do this with their Apples. Similar systems can be rigged so that if a computer is unplugged, the first thing it does upon revival is a purge (not a directory purge which comes with simply deleting file names, a complete reformatting of the disk which erases *all* data). This means, though, that every power failure will have the same effect. It will take some time to make a good system of protection, but this is probably the most constructive project that BBS operators can engage in. It doesn't matter if you have "nothing to hide". The fact is you have everything to protect from intruding eyes. Because when they seize equipment they read everything without concern that the sysop may be the caretaker of people's personal messages and writings.

We'd like to hear other methods of outsmarting these goons. It's not very hard. For instance, you could have a bulletin board dial-in at one location, which will then call-forward to the real location, or still another dummy location. Each of these requires another phone line, but you'll get plenty of warning, especially if a dummy computer is set up at one of the locations. And this is only the beginning.

We don't enjoy having to suggest these courses of action. We'd like very much to be able to get on with what we're supposed to be doing: discussing telecommunications and computers in our own way. Instead we have to pause again to defend our right to say these things. It's a necessary course of action and, if we hold our heads up, it will be a successful one.

PRIVATE SECTOR SEIZED

(continued from page 2-51)

little technical understanding, and in the process they have abused many people's constitutional rights. What we have developing is a mini witch hunt which is analogous to some of the arrests at day care centers, where they sweep in and arrest everybody, ruin reputations, and then find that there is only one or two guilty parties." We feel that law enforcement, not understanding the information on the BBS, decided to strike first and ask questions later.

2600 magazine and the sysops of the Private Sector BBS stand fully behind the system operator. As soon as the equipment is returned, the BBS will be back up. We ask all our readers to do their utmost to support us in our efforts, and to educate as many of the public as possible that a hacker is not a computer criminal. We are all convinced of our sysop's innocence, and await Rockoff's dropping of the charges.

[NOTE: Readers will notice that our reporting of the events are quite different than those presented in the media and by the Middlesex County Prosecutor. We can only remind you that we are much closer to the events at hand than the media is, and that we are much more technologically literate than the Middlesex County Prosecutor's Office. The Middlesex Prosecutor has already taken back many of his statements, after his contentions were disproven by AT&T and the DOD. One problem is that the media and the police tend to treat the seven cases as one case, thus the charges against and activities of some of the hackers has been extended to all of the charged. We at *2600* can only speak about the case of Private Sector.]

STATE OF NEW JERSEY }
COUNTY OF MIDDLESEX } SS SEARCH WARRANT

1. This matter being opened to the Court by Assistant Prosecutor [illegible] on application for the issuance of a search warrant for the [X] premises, [ ] person, [ ] vehicle described below, and the Court having reviewed the [ ] affidavit, [X] testimony under oath, of the said Detective George [illegible] South Plainfield Police Department, and being satisfied therefrom that [illegible] is evidence of violations of the New Jersey Statutes, to wit: NJS 2C:20-25(c) & 2C:2-6 Complicity in computer theft, specifically, computer equipment, including hardware, software, manuals, computer supplies, address books, records, notes, memoranda, phone, phone bills, phone records and correspondence relating to the operation of the computer.

and that probable cause exists for the issuance of such warrant(s).

2. You are hereby authorized to search the [X] premises described below, [ ] person described below, [ ] vehicle described below, and to serve a copy of this warrant on such person or on the person in charge or control of such premises.

3. You are hereby ordered, in the event you seize any of the above-described items [illegible], to give a receipt for the property so seized to the person from whom it was taken or in whose possession it was found, or in the absence of such person to leave a copy of this warrant together with such receipt in or upon the said premises from which the property is taken.

4. You are hereby authorized to enter the premises described below [ ] with, [X] without, first knocking and identifying the officers as police officers and the purpose for being at the premises, if applicable.

5. You are further authorized to execute this warrant between the hours of 9:00 AM and 9:00 PM within [illegible] days from the issuance hereof, and thereafter to forthwith make prompt return to me with a written inventory of the property seized hereunder.

6. The following is a description of the [X] premises, [ ] person, [ ] vehicle to be searched:

Rockaway Township, New Jersey, more specifically described as a one family split level residence with blue aluminum siding, and hedges surrounding the property, with computer located in an upstairs bedroom on the right side.

7. Given and issued under my hand at New Brunswick, Middlesex County, New Jersey, at 2:33 o'clock, P.M. this 11th day of July 19 85.

JUDGE OF THE SUPERIOR COURT
MARTIN KRAWARIK
J.S.C.

EVERYONE KNOWS A QUALITY BULLETIN BOARD SYSTEM WHEN THEY SEE ONE. THAT'S WHAT THE PRIVATE SECTOR WAS—AND WILL BE AGAIN, WITH YOUR HELP. TELL THE WORLD WHAT THE PRIVATE SECTOR WAS ALL ABOUT AND HOW IT WAS UNJUSTLY SNATCHED IN ITS PRIME. WRITE OR CALL YOUR ELECTED OFFICIALS AND OFFER TO EXPLAIN THIS KIND OF THING TO THEM. THEY *WILL* LISTEN BECAUSE NO ONE ELSE IS GOING TO TELL THEM! DONATE YOUR TIME, RESOURCES, AND/OR ABILITIES AND STAY IN TOUCH WITH *2600* AT (516) 751-2600. YOUR IDEAS ARE WELCOME.